Unsolicited Commercial E-mail, Privacy Concerns Related To Social Network Services, Online Protection of Children, and Cyberbullying

USHA MUNUKUTLA-PARKER*

ABSTRACT

Electronic spam or Unsolicited Commercial E-mail ("UCE") refers to the dissemination of identical e-mail advertisements to thousands or more recipients. Spam is extremely cost-effective for those who generate it. However, the cost to Internet Service Providers ("ISPs") – for infrastructure costs for filtering and virus-checking systems, time and cost of handling customer complaints, and wasted network bandwidth and storage capacity – and costs to corporations with company e-mail – for lost productivity in addition to infrastructure and network costs similar to those of ISPs – are astronomical. Congress responded to the growing frustration and losses attributable to spam by passing the CAN-SPAM Act of 2003. In addition, thirty-eight states currently have legislation to curb spam. These laws and related litigation are discussed. While UCE has been a nuisance for several years, an up-and-coming source of online intrusions is social network services. These online clubs serve a wide variety of interests such as professional networking or social interactions. Only some of the services require registration to view the online profiles of other registered members while most provide the opportunity to link from one registered member to another through a friend or associate list. Many of the privacy concerns associated with social network services stem from information voluntarily posted by the registered members themselves. Other problems arise when the services are linked with the registered users' e-mail databases. These problems and the initial attempts to deal with them are discussed in the context of some of the most popular social network services. Both federal and state legislators have recognized and addressed the need to protect children who use the Internet from inappropriate content and information gathering. Federal protection has taken the form of three statutes. First, the Child Online Privacy Protection Act ("COPPA") applies to commercial websites that target children under age thirteen or that have actual knowledge that they are collecting information from a minor, and it mandates several requirements for the collection, use, and disclosure of personal information about

---

* Usha Munukutla-Parker is a J.D. candidate at The Ohio State University Moritz College of Law, class of 2007. Usha holds a B.S. in electrical engineering from Tennessee Technological University and an M.S. in electrical engineering from Virginia Polytechnic & State University.

children. COPPA empowers states' attorneys general to bring civil action against violators of the Act on behalf of state residents. Second, the Child Online Protection Act ("COPA") prohibits the transmission of material to children that is for commercial purposes and may be harmful to minors. The Supreme Court has upheld a temporary injunction on the enforcement of this Act. Finally, the Children's Internet Protection Act ("CIPA") requires schools and libraries to filter online content to prevent minors from being exposed to inappropriate content in order for those facilities to retain federal funds. The constitutionality of this statute has withstood challenge.

A relatively new and growing threat to children online is cyberbullying. Cyberbullying is a form of online harassment that may be accomplished through the posting of cruel or even threatening messages. Unlike cyberharassment or cyberstalking, which involves adults, cyberbullying involves minors on both sides of the harassment. Parents, school officials, and legislators are beginning to take notice of the problem and issues that arise in trying to curtail the practice.

I. UNSOLICITED COMMERCIAL E-MAIL

A. INTRODUCTION

Unsolicited Commercial E-mail ("UCE") has proven to be a persistent problem, presenting a considerable inconvenience to e-mail users and a significant cost to e-mail providers.[1] Spam has become a nuisance for every person with an e-mail account. As recently as May of 2004, end users reported receiving an average of twenty-nine spam e-mails per day.[2] The cost to end users can range from relatively minor, such as the wasted time in verifying and deleting the spam e-mails, to major, such as the triggering of malware in an attempt to opt

---

[1] Saul Hansell, *The High, Really High or Incredibly High Cost of Spam*, N.Y. TIMES, July 29, 2003, *available at* http://www.lexisone.com/balancing/articles/n080003d.html (last visited Sept. 29, 2006). Spam is unsolicited commercial e-mail which is sent to thousands of recipients or more. Wikipedia (E-mail Spam), http://en.wikipedia.org/wiki/E-mail_spam (last visited Sept. 29, 2006). At least some of the persistence of the problem stems from the low cost of generating spam. The cost was estimated as .025 cents per spam e-mail in mid-2003.

[2] *How Has the Can-Spam Act Fared So Far?*, SYMANTEC, Aug. 10, 2004, http://enterprisesecurity.symantec.com/article.cfm?articleid=4480&EID=0 (last visited Sept. 29, 2006).

out of the spam e-mail.[3] Internet Service Providers ("ISPs"), companies with corporate e-mail servers, and other providers of e-mail service have been forced to minimize the detrimental effect of spam on their customers and their networks through substantial investments in infrastructure and software.[4]

By 2003, UCE had become enough of a problem to impel the federal and most state governments to pass legislation to curb the practice and minimize its costs. The federal CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act)[5] took effect at the start of 2004 and imposes requirements like the labeling of spam e-mail and the ability of recipients to opt out of future e-mails.[6] Thirty-eight states also currently have laws to regulate spam.[7] State laws addressing the labeling of spam or prohibiting spam entirely are preempted by the CAN-SPAM Act, but states are free to address the deceptive quality of spam messages.[8]

B. FEDERAL LEGISLATION AND REGULATION

The CAN-SPAM Act is enforced by the Federal Trade Commission ("FTC") and the Department of Justice ("DOJ"), which have congressional authority to enforce criminal sanctions.[9] The Act

---

[3] Wikipedia (Malware), http://en.wikipedia.org/wiki/Malware (last visited Sept. 29, 2006) ("[Malware] is software designed to infiltrate or damage a computer system without the owner's consent."). Computer users can attempt to avoid spam in several ways. Wikipedia (E-mail Spam), http://en.wikipedia.org/wiki/Spam_%28e-mail%29#Avoiding_sending_spam (last visited Sept. 29, 2006).

[4] Hansell, *supra* note 1.

[5] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), 15 U.S.C. §§ 7701-7713 (2005).

[6] Federal Trade Commission, *The CAN-SPAM Act: Requirements for Commercial Emailers* [hereinafter *CAN-SPAM Act*], http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm (last visited Sept. 29, 2006).

[7] Spam Laws, http://www.spamlaws.com/state/index.shtml (last visited Sept. 29, 2006).

[8] "State laws that require labels on unsolicited commercial e-mail or prohibit such messages entirely are pre-empted, although provisions merely addressing falsity and deception would remain in place." CAN-SPAM Act of 2003: Summary, http://www.spamlaws.com/federal/summ108.shtml#s877 (last visited Sept. 29, 2006).

[9] *CAN-SPAM Act*, *supra* note 6.

imposes several requirements on senders of commercial e-mail,[10] and failure to comply with the requirements of the Act can result in monetary sanctions of up to $11,000.[11] Additional sanctions befall spam generators who use certain methods for obtaining or generating the e-mail addresses of recipients.[12] Criminal penalties, including imprisonment, are imposed by the DOJ for certain acts by commercial e-mail senders.[13] The FTC issued criteria for determining "the primary purpose" of a commercial e-mail and promulgated a rule requiring the labeling of sexually explicit commercial e-mail.

Despite the scope of the CAN-SPAM Act and the substantial penalties that can be triggered by non-compliance, the efficacy of the Act seemed limited at the end of 2004, nearly a year after it had been in effect.[14] According to a survey by MX Logic, an anti-spam company, 97 percent of unsolicited commercial e-mail sent in 2004 violated the Act.[15] In addition, the FTC has declined to exercise some of the power granted to it by the CAN-SPAM Act. The FTC could have established a national *do-not-e-mail* registry, similar to the *do-not-call* registry established for unsolicited commercial phone calls.[16]

---

[10] *Id.* The Act bans false or misleading header information so that the origin of e-mails can be accurately ascertained. Deceptive subject lines are prohibited so that the content of an e-mail message is clear. Opt-out mechanisms are required and must be honored. Commercial e-mail must be labeled as an advertisement, and a valid physical address of the sender must be included.

[11] *Id.*

[12] *Id.* E-mail addresses may not be "harvested" from Web sites or services. E-mail addresses may not be generated through a combination of names, letters or numbers. Senders may not use scripts to register for multiple e-mail accounts used to send commercial e-mail. E-mails may not be relayed through a computer or network.

[13] *Id.* Sending commercial e-mail from a computer without authorization is prohibited. Commercial e-mail may not be relayed or retransmitted through one or more computers for the purpose of obfuscating the initial source. Header information in commercial e-mails may not be falsified. The use of false information to register for multiple domain names or e-mail accounts is criminally sanctionable. False representation as the owner of multiple Internet Protocol addresses which are used to send commercial e-mail is also criminally sanctionable.

[14] Paul Festa, *Can-Spam Didn't, Survey Says*, CNET NEWS.COM, Dec. 29, 2004, http://news.com.com/Can-Spam+didnt%2C+survey+says/2100-1030_3-5506976.html?tag=nefd.top (last visited Sept. 29, 2006).

[15] *Id.*

[16] Wikipedia (CAN-SPAM Act), http://en.wikipedia.org/wiki/Can_Spam_Act_of_2003 (last visited Sept. 29, 2006).

However, it rejected the proposal out of concerns over the inability to authenticate e-mail, and, ironically, the possibility of spammers hacking a registry containing e-mail addresses by spammers.[17] In fact, the most significant benefit of the Act seems not to be a reduction in spam that violates the federal law but, rather, in the ability of ISPs to use the law against the most insidious violators.[18]

C. STATE LEGISLATION

The majority of states have passed laws to regulate spam, but any state law provision dealing with the labeling of UCE is preempted by the CAN-SPAM Act.[19] For example, at least twenty-four states have passed laws to specify the text that must appear in the subject line of a commercial e-mail, but such a provision is preempted by the CAN-SPAM Act.[20] Utah repealed its Unsolicited Commercial and Sexually Explicit Email Act which was preempted in large part by the CAN-SPAM Act.[21] State laws that prohibit misleading routing information or misleading subject lines on commercial e-mail are not preempted by the federal law.[22]

---

[17] *Id.*

[18] Microsoft alone has brought multiple suits against spammers who have targeted customers of the MSN portal and Hotmail e-mail service. Matt Hines, *Microsoft Awarded $4 Million in Spam Suit*, CNET NEWS.COM, July 16, 2004, http://news.com.com/Microsoft+awarded+4+million+in+spam+suit/2100-1014_3-5272776.html?tag=nl.

[19] Thirty-eight states have laws to regulate commercial e-mail. Spam Laws: Summary, http://www.spamlaws.com/state/summary.shtml (last visited Sept. 29, 2006).

[20] *Id.* Alaska, Arizona, Arkansas, Colorado, Connecticut, Illinois, Indiana, Kansas, Louisiana, Maine, Michigan, Minnesota, Missouri, Nevada, New Mexico, North Dakota, Oklahoma, Oregon, Pennsylvania, South Dakota, Tennessee, Texas, Utah, and Wisconsin require that specific text, like "ADV" or "ADV: ADULT," appear in the subject line of commercial e-mail.

[21] S.B. 92, 2004 Gen. Sess. (Utah 2004) (repealing UTAH CODE ANN. § 13-36-101 – 105).

[22] Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming prohibit missing or misleading routing information. Indiana, Kansas, Maryland, Minnesota, Missouri, North Dakota, Pennsylvania, South Dakota, Washington, West Virginia, and Wyoming prohibit misleading subject lines in commercial e-mails. Spam Laws, *supra* note 19.

D. LITIGATION AND FILTERING

ISPs have taken a lead in the legal war against spammers. Microsoft had filed approximately sixty spam-related suits by the end of 2004 and won a $4 million award in one case.[23] EarthLink has also successfully brought actions against spammers under the CAN-SPAM Act. The ISP won a multimillion dollar award in one case and money damages as well as jail time for the spammer in another case.[24]

The CAN-SPAM Act has been used both by the FTC and by states without their own spam-regulating laws. Massachusetts became the first state to sue a spammer under the federal statute.[25] The state won a $25,000 award and the Florida-based spammer was ordered to cease sending deceptive unsolicited commercial e-mails.[26] In the first criminal charges filed by the FTC under the CAN-SPAM Act, a defendant group, "Phoenix Avatar," was alleged to send spam e-mail advertising essentially worthless products.[27] The FTC was awarded permanent injunctive relief, and damages were assessed at $20,000.[28] Finally, in addition to the FTC, ISPs, and states, individuals have also joined the battle against spammers.[29]

While litigation has worked to punish some of the worst offenders for disseminating deceptive spam, advancing spam-filtering technology may hold the most promise for actually curtailing the cost and inconvenience associated with spam. The percentage of spam within e-mail has been as high as 94.5% even after the enactment of

---

[23] Hines, *supra* note 18.

[24] Ed Oswald, *Earthlink Continues Spam Legal Battle*, BETA NEWS, Nov. 18, 2005, http://www.betanews.com/article/EarthLink_Continues_Spam_Legal_Battle/1132337813.

[25] Hines, *supra* note 18.

[26] Office of Massachusetts Attorney General Tom Reilly, http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1316 (last visited Sept. 29, 2006).

[27] Wikipedia (CAN-SPAM Act), *supra* note 16.

[28] FTC v. Phoenix Avatar, No. 04C2897, 2004 U.S. Dist. LEXIS 14717 (N.D. Ill., July 29, 2004). Final order announced in Press Release, FTC News, Diet Patch Sellers Settle CAN-SPAM Charges: Operators Marketed Products Via Illegal E-mail Messages (Mar. 31, 2005), http://www.casewatch.org/ftc/news/2005/avatar.shtml (last visited Sept. 29, 2006).

[29] *See* Spamlinks: How to Sue Spammers in the US, http://spamlinks.net/legal.htm#us-sue (last visited Sept. 29, 2006).

CAN-SPAM, but filtering software has been able to prevent up to 68% of that from reaching users' inboxes.[30] The success in preventing the delivery of spam comes at a cost and also at a risk. In addition to the cost of developing and employing the filtering software, companies and ISPs must be vigilant to more sophisticated and targeted spam attacks in retaliation to the filtering.[31] Also, depending on the type of filter used by a company or ISP, the number of false positives, legitimate e-mails that are filtered out as spam, can be significant enough to constitute an added source of inconvenience.[32]

II. PRIVACY CONCERNS RELATED TO SOCIAL NETWORK SERVICES

A. INTRODUCTION

Social Network Services are software programs designed to build and verify social networks for various purposes.[33] Among their broad range of purposes are business-related networking, interaction with people who have common interests, and dating.[34] Users generally enter a profile upon registering with a network and may be able to upload one or more pictures, as well.[35] This profile may be viewed either by a specifically-designated category of users or by any registered or even unregistered user of the site.[36] Some networks

---

[30] Thomas Claburn, *Turning the Tide: Anti-Spam Technologies Help Companies Realize Some Victories in the War Against Junk E-Mail, But There's Still a Long Way to Go*, INFORMATION WEEK, Jan. 17, 2005, http://www.informationweek.com/showArticle.jhtml;jsessionid=JNFGZELXZJ0MKQSNDBCSKH0CJUMEKJVN?articleID=57701581.

[31] See posting of Jeff G. to SpamCop Reporting Help, http://forum.spamcop.net/forums/lofiversion/index.php/t3098.html (Nov. 23, 2004, 3:57 pm).

[32] Heuristic filters are especially susceptible to false positives. *See How Has the Can-Spam Act Fared So Far?*, *supra* note 2.

[33] Wikipedia (Social Network Service), http://en.wikipedia.org/wiki/Social_network_service (last visited Sept. 29, 2006).

[34] Posting of Alberto Escarlate to thesocialsoftwareweblog, *Home of the Social Networking Services Meta List*, http://socialsoftware.weblogsinc.com/entry/9817137581524458/ (Feb. 14, 2005, 5:55 pm).

[35] *See* Christopher Allen, *Overview of Social Network Services*, Life With Alacrity, http://www.lifewithalacrity.com/2003/12/evaluating_soci.html (Dec. 16, 2003, 3:16 pm).

[36] For example, even an unregistered user can go to http://www.friendster.com, enter a registered user's name or e-mail address and, depending on the permissions set by that user, view their profile and their friends.

allow more privacy than others, and this can result in a trade-off with respect to the number of people to whom one can form links within the network.[37] Membership in these services is voluntary, but once registered, members, especially those who expand access to their information to maximize the number of connections they form, may encounter some unpleasant consequences ranging from a slight loss of privacy to the theft of their contact list. Some of the most popular social networking services are featured to highlight concerns associated with the sites.

B. FACEBOOK

Facebook is an online directory that connects people at high schools, colleges, and universities.[38] By the end of 2005, the site had the largest number of registered members among college network sites.[39] Members can register through one of over 25,000 American high schools or with a college or university (.edu) e-mail address.[40] Thus, registered members can be students, alumni, faculty, or staff. Upon registering, members create profiles that can contain as little information as the member's name and e-mail address or much more information, such as the member's major, birth date, political views, sexual orientation, list of friends, or postings by others.[41] Other registered members can view profiles and pictures, post messages to or about the member, and jump to profiles of members listed as friends of the profiled member currently under view. Registered participants can create groups within Facebook or join existing groups either by invitation or on their own. The site allows any registered member to report another member or a group within Facebook for racist or otherwise offensive posts. The site's administrators have the discretion to delete the postings or the related accounts.

---

[37] Allen, *supra* note 35.

[38] Wikipedia (Facebook), http://en.wikipedia.org/wiki/Facebook (last visited Sept. 29, 2006).

[39] *Id.*

[40] *Id.*

[41] *See id.* Items users can include in their profiles and display are: city, gender, concentration, birthday, hometown and state, high school, relationship status, sexual orientation, political views, interests, favorite music, favorite TV shows, favorite movies, favorite books, favorite quotes, and a short self-description of the user.

Facebook offers more interschool privacy than many other college-networking web sites because a registered member cannot view the profile of someone at another school unless that person has already listed them as a "friend" or has "poked" them.[42] The "poke" issues a message to the person who has been poked the next time they log in to Facebook. The site allows members to restrict access to their information and also allows access to be blocked to specified members.[43]

Despite the security options within the site, members who expand access by other members in order to fulfill the networking purposes of the site can encounter unexpected consequences from the loss of privacy. Contact resulting from participation in the site can be somewhat benign or only mildly intrusive, such as a "poke" from a stranger or a friend of a friend. This type of contact can be analogized to non-commercial spam. Other contact may progress to varying degrees of stalking.[44] Perhaps the most unexpected use of information on the Facebook site has been by law enforcement, school officials, and potential employers.[45] Many high schools and the University of

---

[42] *Id.* Although one cannot view the profile of a friend of a friend who attends a different school, one can view that person's "friends" list.

[43] *See id.* Users can restrict access to their information through searches, access to their profile information and contact information. Users can also specify whether other users will have access to their friends list, information about their last login, upcoming events, courses, wall which holds messages from other users, and the list of groups for which the user is a groupie (a group in which the user has many "friends").

[44] *See* Nicole Wetherell, *thefacebook stalkers*, THE GW HATCHETT, March 7, 2005, http://www.gwhatchet.com/media/paper332/news/2005/03/07/Style/Thefacebook.Stalkers-887328.shtml?norewrite&sourcedomain=www.gwhatchet.com. (Another user may repeatedly "poke" the stalking victim and try to increase contact or may anonymously stalk a person on Facebook by visiting their profile and learning everything about them that they choose to post. It sometimes takes an incident of stalking to alert a user to the fact that they have to be careful about the type and amount of information they post).

[45] Wikipedia (Facebook), *supra* note 38. School officials have used Facebook to uncover underage drinking and violations of "dry campus" policies and to investigate other violations of school policy. "In November 2005, four students at Northern Kentucky University were fined for posting pictures of a drinking party on Facebook. The pictures, taken in one of NKU's dormitories, proved that the students were in violation of the university's dry campus policy." In October 2005, a student was expelled from Fisher College for Facebook postings about a campus police officer that were deemed to violate the school's code of conduct. Several campuses have experienced problems with elections due to Facebook postings. For example, election results at the University of Pennsylvania were delayed in October 2005 because Facebook advocacy groups appeared before the date when candidates were permitted to begin campaigning. Wikipedia (Facebook's Use in Investigations),

New Mexico have blocked access to the Facebook site from school computers.[46] While high schools are primarily concerned with the creation of Facebook groups which are essentially hate groups against peers and staff members, the University of New Mexico was also concerned about Facebook's violations of the university's Acceptable Computer Use Policy with respect to spam and trademark infringement.[47]

C. FRIENDSTER

Friendster is an Internet social networking service that is similar in many ways to Facebook. Users register with the site by establishing a profile and then connect to friends and friends of friends. The difference is that Friendster is not limited to schools. Anyone can become a registered member of the site. In addition, even unregistered users can view Friendster profiles depending on the permissions that are set for a given profile.[48] Thus, the concerns raised in the Facebook discussion about both non-commercial spam and stalking are expanded to the population at large. Even an unregistered user can enter a name, school, or hometown as a search term and view profiles that match that search. The fact that the information, voluntarily posted by the registered member, might be of interest to a potential stalker illustrates the tension between privacy concerns and the registered member's desire to fulfill the networking promise of the site. The more information a member reveals and the more lax he or she is with regard to privacy settings, the more likely he or she is to connect with distant friends or friends of friends.

---

http://en.wikipedia.org/wiki/Facebook%27s_use_in_investigations (last visited Sept. 29, 2006). Investigators used the Facebook site to identify students who had run onto the football field during a game. Devon Lash, *Site Used to Aid Investigations*, THE DIGITAL COLLEGIAN, Nov. 10, 2005, http://www.collegian.psu.edu/archive/2005/11/11-10-05tdc/11-10-05dnews-09.asp. Faculty members may view Facebook profiles before writing recommendation letters for students, and alumni at potential employer's companies may use Facebook to screen out candidates. Lauren Morgan, *Facebook Can Hurt Employment Chances*, REDANDBLACK.COM, Dec. 6, 2005, http://www.redandblack.com/vnews/display.v/ART/2005/12/06/439512618c11c.

[46] Wikipedia (Facebook), *supra* note 38.

[47] *Id.*

[48] By going to the site www.friendster.com, anyone can enter the name or e-mail address of a registered user and view their profile and jump to the profiles of their friends.

In an interesting turn-about on those who view profiles of others on Friendster, the site began displaying the list of members who had accessed a given profile in the Fall of 2005.[49] This, too, is a form of privacy breach because registered members who had always felt free to anonymously view other members' profiles were not warned before their activity was tracked and reported. Although registered users can change settings to continue to view profiles anonymously, they cannot remove their names from profiles that were viewed before the change in settings.[50] A serious breach of privacy, which has since been patched, was the ability of Friendster members to secretly obtain profile information about other members who had accessed their profile.[51]

D. MySpace

MySpace is a social network service with largely similar features and vulnerabilities to Friendster. Thus, even non-members can view profiles though their initial access is restricted to only the profiles displayed by the site.[52] One difference is the level of personalization that members can exercise over their profile page. Among the page elements that can be changed are the background, fonts, and cursor. Users can also run scripts to dynamically change the look of their profile page. For example, a user can have photos on the page flip upside-down when the cursor is on them. Inexperienced users running some of these programs have caused system problems.[53] More

---

[49] Post on Berkeley Intellectual Property weblog (bIPlog), http://www.boalt.org/biplog/archives/627 (Sept. 29, 2005, 10:40 pm).

[50] *Id.*

[51] Posting of Matt Chisholm to More Theory, http://more.theory.org/archives/000106.html (May 2, 2004, 1:20 pm). Hackers could link their Friendster profiles with their homepage and run a program on their homepage to receive an e-mail from Friendster containing the name, e-mail address, and user-id of those who visited their profiles.

[52] Friendster, www.friendster.com, allows anybody to enter a member's name, school or hometown and view their profile if that profile's permissions allow. MySpace, www.myspace.com, has two or three profiles on the startup page which anybody can view and through which anybody can connect to friends of that member, but the site does not allow non-members to search for specific profiles.

[53] Wikipedia (MySpace), http://en.wikipedia.org/wiki/Myspace (last visited Sept. 29, 2006). Malformed coding in poorly constructed profiles can freeze browsers like Microsoft's Internet

importantly, the increased personalization capabilities may be partly responsible for some problems with inappropriate content on MySpace.

The type of content allowed on MySpace has led to its increased popularity in some arenas and the barring of the site in others. Amateur bands and would-be porn stars have gained attention through their MySpace profiles.[54] This has led existing media outlets to create their own MySpace profiles.[55] On the other hand, schools and libraries are among entities that have restricted access to the site.[56] The vulnerability of underage users within MySpace has led to a highly publicized lawsuit as well as a House Bill banning the use of social network services in public places such as libraries.[57]

In addition to child predators, hackers have also presented problems for the MySpace site. MySpace had been vulnerable to the problem described in the discussion of Friendster whereby a member's profile could be linked to a homepage that ran a script to receive information from the site about other members who accessed the profile.[58] Like Friendster, MySpace has closed this loophole.[59] In July of 2005, another vulnerability of MySpace, less related to privacy than inconvenience, had been publicized, and by October, a member exploited it to create a worm that added over a million profiles to his buddy list and forced the site to shut down for maintenance.[60]

Explorer. Videos and other high bandwidth objects could corrupt the program if it is simultaneously playing another file from the user's computer.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.* The American Library Association views the House Bill, Deleting Online Predators Act ("DOPA"), as redundant in light of the Children's Internet Protection Act ("CIPA"). *DOPA Passes House by Wide Margin; ALA Dismayed*, LIBRARY JOURNAL.COM, July 28, 2006, http://www.libraryjournal.com/article/CA6357145.html.

[58] Chisolm, *supra* note 51.

[59] *Id.*

[60] Wikipedia (Samy), http://en.wikipedia.org/wiki/Samy_(XSS) (last visited Sept. 29, 2006).

E. PLAXO

Plaxo is an online address book service that provides automatic updating of contact information.[61] Members and their contacts store information on Plaxo's servers.[62] When any member changes some of the information in his or her contact list, it is automatically updated in every Plaxo-stored address book in which it appears.[63] Thus, the most convenient scenario for Plaxo members is if all of their contacts join Plaxo as well. One source of online intrusion from this site has been repeated requests from Plaxo members to their contacts asking that they update their information.[64] These e-mails from Plaxo are seen by some as annoying and by others as spam.[65] A more serious concern about Plaxo has stemmed from the storage of members' contact information on Plaxo servers. When company employees use Plaxo, the connection between Plaxo and the employee's e-mail contacts has been regarded as a breach of many companies' data privacy policy.[66] This is because most companies have policies that protect client lists. In addition, many companies regard their own employee list as private and confidential. An employee's e-mail list at many companies will link to every other employee within the company. Aside from raising privacy concerns stemming from its link to members' contact lists, Plaxo also raises legitimate concerns about the vulnerability of the information stored on its servers to theft by spam generators.

F. LINKEDIN

LinkedIn is a social network service focused on business connections.[67] The site shows the "degrees of separation" between a

---

[61] Wikipedia (Plaxo), http://en.wikipedia.org/wiki/Plaxo (last visited Sept. 29, 2006).

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] Cara Garretson, *Address Book Apps Try to Shake Spam Label*, NETWORK WORLD, Aug. 9, 2004, http://www.networkworld.com/news/2004/080904specialfocus.html.

[66] Linda Musthaler, *Leave Social Networks at Home*, NETWORK WORLD, Sept. 13, 2004, http://www.networkworld.com/columnists/2004/091304musthaler.html.

[67] Wikipedia (LinkedIn), http://en.wikipedia.org/wiki/Linkedin (last visited Sept. 29, 2006).

member and any other member on the site and offers more security from communication from other members than many other sites because of its "gated-access approach."[68] "Gated-access approach" refers to the fact that members of LinkedIn can only connect to one another through a mutual contact and by mutual consent. If you search and find a member whom you already know, you must enter their e-mail address yourself to contact them outside the context of an introduction through a mutual friend. Thus, non-commercial spam is much less of a concern within LinkedIn than in other social network services.

HR professionals have begun to use LinkedIn to determine the connections between themselves and potential candidates for employment at their companies.[69] Early in 2005, LinkedIn added a service to allow members to post job listings on the site.[70] Other members submit resumes and applications through contacts of the member who posted the job opening.[71] An advantage of this approach for employers is that candidates are much less prone to padding their qualifications when they know that their profile is available for view by their co-workers and former employers.[72] Also, employers receive every resume only through a known contact.[73] Despite its advantages, this service could prove to be a privacy concern for employees if HR professionals begin to view LinkedIn primarily as a job search engine and regard the presence of their current employees on the membership roster as a sign that they are seeking employment elsewhere.[74]

Another source of concern about the LinkedIn site is the option for a member to upload all or a selected subset of a user's Microsoft Outlook contact list to the site to determine which of the contacts are already LinkedIn members.[75] The feature is a convenient way to

---

[68] *Id.*; Jennifer C. Berkshire, *'Social Network' Recruiting*, SOC'Y FOR HUMAN RES. MGMT., Apr. 2005, http://www.shrm.org/hrmagazine/articles/0405/0405berkshire.asp.

[69] Berkshire, *supra* note 68.

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Berkshire, supra note 68.*

establish more contacts within the network, and the site does not allow contacts to appear in search results until, and unless, they have agreed to join.[76] However, as with Plaxo, the feature elicits legitimate fears about contact lists becoming compromised to spam generators through a security breach.

G. CONCLUSION

The preceding discussion illustrates the variety of purposes for social network services. While the sites are an increasingly popular means for getting back in touch with old friends, meeting new friends, and making business contacts, each type of site has its share of privacy concerns. In many cases, these concerns are directly proportional to the amount of private information registered members themselves choose to display online. The trade-off that most sites offer between increased privacy and decreased ability to connect with other members presents a tension for registered members who would like to reap the full benefit of their membership to connect with as many people as possible. Unfortunately, potential employers or even stalkers have access to the same personal information as friends and colleagues. In addition, services that link members' e-mail lists to their server may not only violate those members' company policies but also inadvertently lose the lists in security breaches by spammers. Ultimately, awareness by members of social network services that any information they choose to reveal on the site could potentially be viewed by anyone–friend or foe–would go a long way in curtailing some of the privacy issues.

III. LEGAL UPDATE: ONLINE PROTECTION OF CHILDREN

A. INTRODUCTION

The protection of children on the Internet falls to three federal statutes designed to curtail both the downloading of inappropriate content to children and the uploading of impermissible personal information from children. In addition, two states have recently passed controversial laws creating a children's e-mail registry.

---

[76] *Id.*

B. FEDERAL LEGISLATION

The broadest of the federal statutes, Child Online Privacy Protection Act ("COPPA"), has been in effect since 2000.[77] COPPA is administered by the Federal Trade Commission ("FTC") and is directed to the protection of children under thirteen from operators of commercial Web sites or online services.[78] COPPA mandates several requirements for sites that either direct their services to children under thirteen or have actual knowledge that their general audience site is collecting information from children under thirteen.[79] The Act applies to individually identifiable information about children and requires, among other things, that sites post a clear notice of their data collection practices on their home page and on every page where information is requested.[80] COPPA creates an exception for children's e-mail addresses collected for such uses as contests, online newsletters, homework help, and online postcards.[81] Also, COPPA contains a safe harbor provision for site operators who comply with Commission-approved self-regulatory industry guidelines.[82] The FTC solicited comments from the public in early 2005 for a report it must submit to Congress after reviewing the Act.[83]

Another federal statute, Child Online Protection Act ("COPA"), restricts "access by minors to materials commercially distributed by means of World Wide Web that are harmful to minors."[84] Enforcement of this statute is currently enjoined by the Supreme Court, which upheld a temporary injunction by the Third Circuit Court

---

[77] Child Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2000).

[78] FTC, How to Comply With The Children's Online Privacy Protection Rule, http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm (last visited Sept. 29, 2006).

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] Press Release, FTC, FTC Seeks Comment on Children's Online Privacy Rule (Apr. 21, 2005), http://www.ftc.gov/opa/2005/04/coppacomments.htm.

[84] Child Online Protection Act ("COPA"), 47 U.S.C. § 231 (2005).

of Appeals.[85] Finally, the narrowest statute, Children's Internet Protection Act ("CIPA"), applies only to public libraries and schools and mandates that they employ software filters to restrict access by minors to inappropriate material.[86] CIPA has withstood challenge to its constitutionality.[87]

C. STATE LEGISLATION

Utah and Michigan have recently enacted laws to protect children from inappropriate spam.[88] Both states allow parents and schools to register e-mail addresses that are accessible to children. Businesses are prohibited from sending inappropriate sales e-mails to addresses on the list within thirty days of the address' placement in the registry.[89] Both states have faced mounting opposition to these laws, and even the FTC has said that the "registries pose serious 'security and privacy risks.'"[90] Among the risks is access to the registry lists by online predators.[91]

D. LITIGATION

COPPA is the only statute under which federal litigation has taken place to date. Two of the biggest fines for COPPA violations were imposed on UMG Recordings ($400,000) and Bonzi Software

---

[85] *See* Ashcroft v. ACLU, 542 U.S. 656 (2004); *see also* CDT Policy Post, http://www.cdt.org/publications/pp_8.11.shtml.

[86] Children's Internet Protection Act ("CIPA"), 20 U.S.C. § 9134(f) (Library Services and Technology); *see also* 47 U.S.C. § 254(h)(6) (Discounts from telecommunication service companies to compliant schools and libraries.).

[87] United States v. Am. Library Ass'n, 539 U.S. 194 (2003).

[88] David Kesmodel, *Protecting Kids From Adult Spam*, WALL ST. J. ONLINE, January 12, 2006, *available at* http://www.commercialexploitation.org/news/adultspam.htm (last visited Sept. 29, 2006).

[89] *See generally id.*

[90] *Id.*

[91] *Id.*

($75,000).[92] COPA is currently enjoined from enforcement, and CIPA has not been the basis of action against a school or library as of yet. The two state laws enacted last year have also not been the basis for litigation. At the same time that other states are looking into enacting similar laws, industry groups have begun to challenge the current laws in court.[93]

VI. THE GROWING MENACE OF CYBERBULLYING

Bullying is a ubiquitous and increasingly recognized problem. Bullying can be defined in many ways but is, at its core, a grab for control by the bully through the humiliation of a targeted victim.[94] Bullying is prevalent in schools, workplaces, and society in general.[95] Bullying in schools has taken the form of physical abuse, rumors, teasing, and exclusion from a group.[96] The consequences to victims can include a greater propensity for depression, anxiety, and violent behavior.[97]

"Cyberbullying is sending or posting harmful or cruel text or images using the Internet or other digital communication devices."[98] While bullying can involve adults or children as bullies and victims, cyberbullying, by definition, involves minors on both sides.[99] Essentially, the harassment to which children might have been subjected at school has grown in severity and in reach by way of the

---

[92] Roy Mark, *FTC Fines COPPA Violators*, INTERNETNEWS.COM, February 19, 2004, http://www.internetnews.com/bus-news/article.php/3315291.

[93] Kesmodel, *supra* note 88.

[94] Canada Safety Council, *Bullying in the Workplace*, http://www.safety-council.org/info/OSH/bullies.html (last visited Sept. 29, 2006).

[95] *Id.*

[96] U.S. Department of Health and Human Services, *Stop Bullying Now, at* http://stopbullyingnow.hrsa.gov/index.asp?area=whatbullyingis (last visited Sept. 29, 2006).

[97] Helen Phillips, *Effects of Bullying Worse for Teens*, NEWSCIENTIST.COM, Oct. 29, 2004, http://www.newscientist.com/article.ns?id=dn6600.

[98] *Cyberbullying: Mobilizing educators, parents, students, and others to combat online social cruelty*, http://www.cyberbully.org/ (last visited Sept. 29, 2006).

[99] *Stop Cyberbullying*, http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html (last visited Sept. 29, 2006).

Internet. Incidents of cyberbullying are alarmingly more cruel and dangerous than the types of acts one might associate with traditional bullying. The increased scope of cyberbullying, in terms of the expanded audience and the ability to torment a victim anywhere, presents unique problems not generally associated with bullying. Cyberbullying and its differences from typical school bullying are examined.

A. INTENSITY AND REACH OF CYBERBULLYING

By way of the Internet, a bully may be more brutal than he or she would dare, or care to be, in person.[100] This phenomenon of cyberbullying is attracting more participants and a higher degree of cruelty by participants than traditional schoolyard bullying. Cyberbullying can feel relatively more anonymous and impersonal for the bully.[101] A student who may have reservations about saying something unkind to a fellow student, friend, or former friend in person can take advantage of the anonymity offered by a screen name to post the same comment on an online journal ("blog") or Web site.[102] A cyberbully might even post inflammatory content about the victim for the purpose of eliciting an angry response so the bully can then report the victim for violation of the terms of service rules of a site.[103] Cyberbullies, often teenagers already dealing with typical issues of impulse control, can inflict pain without having to see its effects.[104]

---

[100] Amy Harmon, *Internet Gives Teenage Bullies Weapons to Wound From Afar*, N.Y. TIMES, Aug. 26, 2004, http://www.nytimes.com/2004/08/26/education/26bully.html?pagewanted=1&ei=5090&en=75fcc217518a0daf&ex=1251172800&partner=rssuserland.

[101] *Id.*

[102] *Id.* An elementary school psychologist in Ohio has heard complaints by children who read comments about their weight and clothes online. Counselors have said that "boys make many more explicit sexual comments online than off."

[103] Internet Super Heroes, http://www.internetsuperheroes.org/cyberbullying/index_2.html (last visited Sept. 29, 2006) (Internet Super Heroes is a web site sponsored by Wired Safety, an organization designed to protect individuals online from online crimes, including harassment, stalking, and child pornography. These types of cyber attacks are referred to as "notify" and "warning" wars) [hereinafter Internet Super Heroes (1)].

[104] The sense of detachment can lead to extreme cases like one of a boy who was dared to commit suicide by a group of girls via instant messages ("IMs") and shot himself one day. Center for Safe and Responsible Internet Use, *A Parent's Guide to Cyberbullying and Cyberthreats*, http://cyberbully.org/docs/cbctparents.pdf (last visited Sept. 29, 2006). A 13-

The same bad judgment and lack of impulse control leads school-age children to generate and send some of the very content, often of a sexual nature, about themselves to another student whom they later regret trusting.[105] The sexual content of cyberbullying is especially disturbing in light of its potentially world-wide audience. The sexual harassment and sexual content in cyberbullying may get the attention of adult sexual predators, or cyberbullies may even post ads to offer predators sex with the victim of the bullying.[106] A cyberbully might post an invitation to a pedophile posing as the victim,[107] or register the victim on pornographic web sites or spam e-mail lists.[108]

Perhaps the most painful aspect of cyberbullying for victims is its pervasive reach into their lives.[109] Victims of traditional bullying may skip school to avoid the torment.[110] While staying home is not an effective or long-term solution, it may offer some respite from the pain that victims feel. By contrast, with cyberbullying, there is no longer a

---

year-old had been bullied online and at school for months before he succumbed to his depression and killed himself. His last IM read "Tonight's the night" to which the reply was "It's about time." M. Mindy Moretti, *Playground Bullying Heads to Cyberspace*, COUNTY NEWS ONLINE, Jan. 31, 2005, http://www.naco.org/CountyNewsTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=15014.

[105] Harmon, *supra* note 100 (an 8th grade girl sent a digital video of herself masturbating to a boy she liked who then posted it on a file-sharing network. A 15-year-old e-mailed a nude picture of herself to her boyfriend who forwarded it to his friends. A boy's video serenade to a girl he liked was posted online by her).

[106] *Stop Cyberbullying*, *supra* note 99.

[107] Two 11-year-old girls posing as a 13-year-old neighbor connected with an older man online and gave him the 13-year-old's contact information. The 13-year-old did not even realize her information had been compromised until she received e-mail from the man. Joyce Pellino Crane, *Internet Bullying Hits Home for Teen*, THE BOSTON GLOBE, June 30, 2005, http://www.boston.com/business/personaltech/articles/2005/06/30/internet_bullying_hits_home_for_teen/?page=1; Internet Super Heroes, http://www.internetsuperheroes.org/cyberbullying/summit_8feb05_2.html (last visited Sept. 29, 2006) [hereinafter Internet Super Heroes (2)].

[108] Internet Super Heroes (1), *supra* note 103.

[109] The Association of Educational Publishers, *Cyberbullying: Technology Provides New Channel for Harassment*, http://www.edpress.org/industryinfo/newsletter/techarchives/cyberbullying.htm (last visited Sept. 29, 2006).

[110] U.S. Department of Health and Human Services, *Stop Bullying Now*, http://stopbullyingnow.hrsa.gov/index.asp?Area=effects (last visited Sept. 29, 2006).

"safe" place for a victim. While an obvious solution might appear to be victims going offline, cyberbullying can affect victims without their having read a word of the online content. As discussed, victims of cyberbullying might find that they were made the target of sexual predators.[111] Even if the victims themselves avoid the online content, they may be humiliated to find that friends and family members have seen vicious rumors and lies posted about them.[112] Cyberbullies may post or forward content posing as the victims so that victims experience the consequences of these acts regardless of their awareness of them.[113]

B. EFFORTS AND OBSTACLES TO CURTAILING CYBERBULLYING

For many reasons, some unique to its medium and reach, cyberbullying is an issue that requires a multipronged approach to a solution.[114] More often than not, traditional bullying takes place in schools or on the way to and from school.[115] Thus, schools can develop rules and regulations to prohibit the activity and punish those who defy them. Dealing with cyberbullying presents an additional challenge to schools because the offensive behavior generally occurs outside of school.[116] Schools have been sued for attempting to discipline cyberbullies who used non-school computers during non-school hours to perpetuate their torment.[117] Schools have even

---

[111] Internet Super Heroes (2), *supra* note 107.

[112] Crane, *supra* note 107 (while a high school student was on a school trip to Costa Rica, a group of girls posted sexually explicit journal entries in her name on a popular web site. The girl's sister discovered the postings).

[113] Harmon, *supra* note 100.

[114] Internet Super Heroes (2), *supra* note 107 (one example of the recognition of the complexity of the problem is Westchester County, NY's efforts toward a "multi-pronged educational and awareness campaign against cyberbullying.").

[115] University of New Hampshire Cooperative Extension, *Take A Stand Against Bullying*, http://extension.unh.edu/News/New81304.htm (last visited Sept. 29, 2006).

[116] Internet Super Heroes (2), *supra* note 107 ("Schools have very limited authority to react to things that take place off school grounds, outside of school hours and don't directly impact the school itself.").

[117] *Id.* Schools that have intervened in cyberbullying have lost lawsuits brought by civil liberties groups and parents.

resorted to pressuring students to leave for egregious acts when they lack authority to suspend or punish in another way.[118] School officials are more free to act when school equipment is involved or when the bullying behavior enters the school building.[119]

While schools' efforts to punish cyberbullies may be met with legal battles, their efforts to educate students about proper behavior and Internet use are seen as critical.[120] Schools are increasingly recognizing the need to address cyberbullying issues. In addition to educating children about the Internet, some schools are taking a more holistic approach, viewing cyberbullying as an affront to the community as a whole.[121] Along with educating children to decrease the incidents of cyberbullying, schools are attempting to bring the practice under their purview by establishing new bullying policies that encompass cyberbullying. Armed with these policies, schools can punish violators even for behavior outside of school.[122]

---

[118] Harmon, *supra* note 100 (a sophomore at Fieldstone High School in Bronx, NY agreed not to return to the school after a racist comment she sent to a friend via IM was circulated throughout the school).

[119] Odvard Egil Dyrli, *Cyberbullying: Online Bullying Affects Every School District*, http://www.districtadministration.com/page.cfm?p=1243 (last visited Sept. 29, 2006). In Massachusetts, "after several students in the Boston Public Schools used school computers to send e-mail threats, pornography and simulated hit lists to staff and students, superintendent Thomas W. Payzant banned the district-wide access to Yahoo Mail, MSN Hotmail and other personal e-mail accounts that could not be monitored . . . . Other districts have tried banning or limiting the use of IM, cell-phone text messages and the use of camera phones."

[120] Internet Super Heroes (2), *supra* note 107.

[121] Joan E. Lisante, *Cyber Bullying: No Muscles Needed*, Connect for Kids, June 6, 2005, http://www.connectforkids.org/node/3116. (At Gillispie School in San Diego, the need for a strategy to deal with cyberbullying became clear when Internet threats between some students at the school and a student at another school manifested themselves in physical form with Gillispie students going to the other school to confront the other student. An elementary education coordinator for a counseling organization in Pennsylvania has noted increased requests for inclusion of topics like e-mail and IMs in her regular school bullying sessions. Harmon, *supra* note 100. At the William Penn School in Philadelphia, Pennsylvania, the dean of students emphasizes the view of cyberspace as an extension of the school community while educating students about the pitfalls of a false sense of anonymity online. The school also attempts to bolster the students' own conscience with gentle reminders about their behavior. For example, a mirror in the computer lab has a sign reading "Are you a cyber bully?").

[122] Dyrli, *supra* note 119.

Parents of both bullies and victims are another prong in the effort to deal with cyberbullying.[123] Parents can easily be unaware of the existence or extent of cyberbullying until extreme consequences result, because victims are often less than forthcoming with parents about their predicament.[124] However, parents who are aware and educated about the issue can be instrumental in the safe use of the Internet by their children.[125]

Ironically, Web-based technology is yet another prong in developing some of the solutions to cyberbullying. For example, Internet Service Provider America Online ("AOL") has developed "AOL Guardian" which monitors and reports children's online activity to their parents and restricts those with whom children can have IM chats.[126] Yahoo and Microsoft also offer tools that allow parents to limit online content available to their children.[127] Even online social network services aimed at high school age children have recognized and attempted to deal with the problem of cyberbullying.[128]

Finally, state and national legislation also constitutes a prong in the efforts to curtail cyberbullying.[129] A bill was introduced in the House

---

[123] Internet Super Heroes (2), *supra* note 107 (victims of bullying in school may be cyberbullies themselves. Thus, there is no clear demarcation between perpetrators and victims).

[124] Joan Whitely, *When Teasing Isn't Funny: The Cost of Bullying*, REVIEW-JOURNAL, October 31, 2005, http://www.reviewjournal.com/lvrj_home/2005/Oct-31-Mon-2005/living/4038822.html. (parents of Ryan Halligan, a 13-year-old who committed suicide after months of online and offline bullying, were unaware of the extent of the torment Ryan had been suffering until after his death).

[125] Lisante, *supra* note 121. Parents who are aware that their children could be cyberbullies or victims or both without their knowledge can be more vigilant in their efforts to educate their children as well as themselves about the techniques and suggested remedies to the issue. Parents are encouraged to learn more about Internet technologies and even develop unacceptable use policies within families. Parents can also employ online tools to monitor and protect their children online.

[126] *Id.*

[127] *Id.*

[128] Sconex, *Information for Parents, Teachers, and School Administrators*, http://www.sconex.com/content/parent_teacher_school_info.php (last visited Sept. 29, 2006).

[129] States are rated based on their legislative efforts to stop bullying and cyberbullying. Bully Police –State Rankings, http://www.bullypolice.org/survey_stats.html (last visited Sept. 29, 2006).

of Representatives in January of 2005 to amend existing safe-school legislation to include bullying and gang prevention.[130] This bill focuses on educational efforts to prevent the problems but does not specifically address cyberbullying. States have dealt with the problem of bullying to varying degrees.[131] Washington State is currently working to pass a cyberbullying law, but that law would only apply to Internet bullying if a school computer were involved.[132] Vermont passed a law dealing with bullying in 2005, but it, too, is silent about cyberbullying.[133] Although communities and schools are becoming increasingly aware of the scope and effects of cyberbullying, it would seem that legislation is still focused on traditional school-based bullying for the most part.

---

[130] Bullying and Gang Prevention for School Safety and Crime Reduction Act, H.R. 283, 109th Congress (2005), *available at* http://www.govtrack.us/congress /bill.xpd?tab=summary&bill=h109-283.

[131] Brenda High, *Making the Grade: How States "Graded" on Their Anti Bullying Laws,* BULLY POLICE USA, http://www.bullypolice.org/grade.html (last visited Sept. 29, 2006). An organization created by the parents of a boy who committed suicide in part because of the trauma of persistent bullying at school tracks bullying-related legislation in states and rates the laws that are developed. The organization views a clear definition of the problem addressed by the law as a key to its efficacy.

[132] Washington State Anti Bullying Law, http://www.bullypolice.org/wa_law.html (last visited Sept. 29, 2006).

[133] John Halligan, *Vermont's New Bully Prevention Law,* http://www.bullypolice.org/RyansLaw.pdf (last visited Sept. 29, 2006) (Rep. Young voted for the Vermont bullying law, H.629). In reference to a Vermont bill on bullying, a state representative noted, "[t]he childhood poem 'sticks and stones will break my bones, but names will never hurt me,' is hereby repealed."